REMARKS

Applicants appreciate the thorough examination as reflected in the Official Action mailed December 3, 2002. Applicants also appreciate the indication of allowable subject matter in Claims 6-8, 19-21 and 32-34. Applicants have amended the specification to incorporate the serial number of the related application. Applicants have amended Claims 1, 14 and 27 to recite "a potential range" rather than "the potential range."

The IDS's

Applicant wishes to bring to the Examiner's attention the IDS's filed August 4, 1999, and June 2, 1999. A copy of the PAIR printout showing receipt of the IDS materials is also provided herewith. Applicants would appreciate the return of initialed PTO-1449 forms for Applicants' previous IDS submissions. For the Examiner's convenience, copies of the PTO-1449 forms are provided herewith.

The Section 102 Rejections

Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56 and 57 stand rejected under 35 U.S.C. § 102 as anticipated by United States Patent No. 4,878,246 to Pastor *et al.* (hereinafter "Pastor"). In particular, the Official Action cites to Pastor, col. 2, lines 6-42 as disclosing each of the recitations of Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56 and 57. Claims 1, 14, 27, 40, 46 and 52 are independent claims. Claims 14 and 27 are system and computer program product claims having recitations corresponding to Claim 1. Claims 46 and 52 are system and computer program product claims having recitations corresponding to Claim 40. Thus, Applicants will address the rejections with reference to Claims 1 and 40, however, analogous arguments apply with respect to Claims 14, 27, 46 and 52. Applicants will first address the rejections of the independent claims and then address the rejections of the dependent claims.

Applicants initially note that certain embodiments of the present invention provide for generating prime values for RSA key generation. RSA keys are discussed in the Background of the present and are generated based on two random large prime numbers. Specification, p.

2, lines 14-28. Claim 1, for example, recites operations for the determination of these prime numbers. In particular, Claim 1 recites:

> 1. (Original) A method of generating an RSA cryptographic value, the method comprising the steps of:
> obtaining user specific information about a user; and
> dividing a potential range of RSA prime values into at least two subintervals;
> selecting a first user-dependent RSA prime from a range of RSA prime values in a first of the at least two subintervals corresponding to a user specific range of values based on the user specific information mapped onto the first subinterval.

Claim 14, likewise, recites:

> 14. (Original) A system for generating an RSA cryptographic value, comprising:
> means for obtaining user specific information about a user; and
> means for determining a user specific range of values based on the user specific information;
> means for dividing a potential range of RSA prime values into at least two subintervals;
> means for mapping the user specific range of values onto a first of the at least two subintervals; and
> means for selecting a first user-dependent RSA prime from the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values.

Similar recitations are found in Claim 27. Applicants submit that the recitations of Claim 1 are not disclosed or suggested by Pastor for the reasons discussed below.

Pastor does not relate to the generation of RSA cryptographic values or to the generation of an RSA prime value for generating RSA keys but, instead, relates to generating memory addresses to extract a key value that is stored in a memory array. Pastor, Abstract ("[t]he ordered pairs of first and second numbers generated correspond to addresses of a memory at which bits of the key are stored."). Memory addresses are not RSA prime values as recited in Claim 1.

Furthermore, Pastor does not disclose "dividing a potential range of RSA prime values into at least two subintervals." While Pastor does recite calculating N values based on a first polynomial and N values based on a second polynomial where the coefficients of the polynomials are derived from an identification number, there is no indication in the cited portion of Pastor that a range of potential RSA prime values, or any other values, is divided into subintervals. Pastor, col. 2, lines 2-59.

Pastor also does not disclose selecting user-dependent RSA prime values. The cited portion of Pastor does not disclose or suggest selection of any prime values but describes the generation of memory addresses from which a key can be extracted. Pastor, col. 2, lines 2-59. There is no indication that any of the generated values of Pastor are prime values other than by chance and, as such, cannot provide for the selection of RSA primes as recited in Claim 1.

In light of the above discussion, Applicants submit that the memory address generation of Pastor neither discloses nor suggests the RSA prime generation operations recited in Claims 1, 14 and 27. Accordingly, Applicants submit that Claim 1, 14 and 27, as well as the claims that depend from them, are patentable over Pastor.

Pastor is also cited as disclosing each of the recitations of independent claims 40, 46 and 52. Claims 40, 46 and 52 provide for selecting cryptographic ranges that are different for different entities. For example, Claim 40 recites:

> 40. (Original) A method of generating a cryptographic value corresponding to a source entity, the method comprising the steps of:
> obtaining entity specific information associated with the source entity;
> selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity.

Similar recitations are found in Claims 46 and 52. Applicants respectfully submit that the recitations of Claims 40, 46 and 52 are not disclosed or suggested by Pastor.

As discussed above, Pastor provides for generating memory address where a key is stored in a memory array. Pastor does not, for example, provide for selection of a cryptographic value from an entity specific range of cryptographic values that are disjoint with ranges of cryptographic values associated with other entities as recited in Claim 40. Thus, in Claim 40, each entity has its own unique range of cryptographic values that is non-overlapping with ranges of other entities. Even if the memory addresses of Pastor are somehow interpreted as being a "range of cryptographic values," there is no indication that such memory addresses are disjoint for different IDs. For example, two different IDs may generate at least some common memory addresses. Accordingly, Applicants submit that the cited portions of Pastor do not disclose or suggest "selecting a cryptographic value from a range of cryptographic values based on the entity specific information, wherein the range of cryptographic values based on the entity specific information is disjoint with ranges of cryptographic values associated with entity specific information associated with entities other than the source entity" as recited in Claims 40, 46 and 52. Applicants, therefore, submit that Claim 40, 46 and 52, as well as the claims that depend from them, are patentable over Pastor.

With regard to the dependent claims, Applicants submit that the dependent claims are patentable as depending from a patentable base claim. However, certain of the dependent claims are also separately patentable over Pastor. For example, Claim 2 recites "selecting a second user-dependent RSA prime from a range of RSA prime values in a second of the at least two subintervals, different from the first subinterval, corresponding to the user specific range of values based on the user specific information mapped onto the second subinterval." Claims 15 and 28 recite "means for mapping the user specific range of values onto a second of the at least two subintervals, different from the first of the at least two subintervals" and "means for selecting a second user-dependent RSA prime from the range of RSA prime values in the second of the at least two subintervals corresponding to the mapped user specific range of values." Applicants submit that selection of RSA prime values from two different subintervals is not disclosed or suggested by the cited portions of Pastor. Accordingly, Applicants submit that Claims 2, 15 and 28 are separately patentable for at least these additional reasons.

Claims 3, 16 and 29 recite that the user specific range values are mapped linearly onto the first subinterval. Applicants submit that such a linear mapping is not disclosed or suggested by the cited portions of Pastor. Accordingly, Applicants submit that Claims 3, 16 and 29 are separately patentable for at least these additional reasons.

Claims 4, 17 and 30 recite that the same mapping function is used to map the user specific range of values onto the first subinterval and onto the second subinterval. Applicants submit that use of the same mapping function to map a user specific range of values onto two different subintervals is not disclosed or suggested by Pastor. Accordingly, Applicants submit that Claims 4, 17 and 30 are separately patentable for at least these additional reasons.

Claims 5, 18 and 31 recite generating a user-dependent RSA key value from the first and second user-dependent primes. Applicants submit that the cited portions of Pastor does not describe the generation of an RSA key and, therefore, does not disclose or suggest the recitations of Claims 5, 18 and 31. Accordingly, Applicants submit that Claims 5, 18 and 31 are separately patentable for at least these additional reasons.

In light of the above discussion, Applicants respectfully submit that Claims 1-5, 9, 14-18, 22, 27-31, 35, 40, 44-46, 50-52, 56 and 57 are not anticipated by Pastor.

<u>The Section 103 Rejections</u>

To establish a prima facie case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. M.P.E.P. §2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). The Court of Appeals for the Federal Circuit has also stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

Claims 10, 11, 23, 24, 36, 37, 41, 42, 47, 48, 53 and 54 stand rejected as obvious under 35 U.S.C. § 103 based on the combination of Pastor and United States Patent No. 5,680,460 to Tomko *et al.* (hereinafter "Tomko"). Applicants submit that each of Claims 10, 11, 23, 24, 36, 37, 41, 42, 47, 48, 53 and 54 are patentable as depending from a patentable base claim.

Claims 12, 13, 25, 26, 38 and 39 stand rejected as obvious under 35 U.S.C. § 103 based on the combination of Pastor and United States Patent No. 6,226,383 to Jablon (hereinafter "Jablon"). While Applicants submit that each of Claims 12, 13, 25, 26, 38 and 39 are patentable as depending from a patentable base claim, Applicants further submit that certain of the dependent claims are separately patentable over the cited references.

For example, Claims 12, 25 and 38 each recite "selecting a random point in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values" and "utilizing the random point as a starting point for a search for a prime number (p) in the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values." Claims 13, 26 and 39 further recite "determining if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values", "selecting a new random point as a search starting point if a candidate for p is considered outside the range of RSA prime values in the first of the at least two subintervals corresponding to the mapped user specific range of values" and "restarting the search for p utilizing the new random point."

The Official Action states that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to select the prime number of Pastor in the manner of Jablon in order to increase computational efficiency as taught in Jablon." Official Aciton, p. 4. However, as discussed above, Pastor does not disclose selection of prime number but describes selection of memory addresses where a key value is stored. As such, the combination of Jablon and Pastor would not result in the recitations of Claims 12, 13, 25, 26, 38 and 39. Furthermore, the motivation for combining Jablon and Pastor is the type of conculsory assertion that the Federal Circuit has found insufficient to establish a prima facie case of obviousness. Accordingly, Applicants submit that Claims 12, 13, 25, 26, 38 and 39 are separately patentable over the cited references for at least these additional reasons.

Claims 43, 49 and 55 stand rejected as obvious under 35 U.S.C. § 103 based on the combination of Pastor and United States Patent No. 5,709,114 to Dawson *et al.* (hereinafter "Dawson"). Applicants submit that each of Claims 43, 49 and 55 are patentable as depending from a patentable base claim.

Conclusion

In light of the above discussion, Applicant submits that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to our Deposit Account No. 09-0461.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

Customer Number:
20792
PATENT TRADEMARK OFFICE

CERTIFICATE OF MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231 on February 28, 2003.

Traci A. Brown
Date of Signature: February 28, 2003

UNITED STATES PATENT AND TRADEMARK OFFICE

Home | Index | Search | System Alerts | eBusiness Center | News & Notices | Contact Us

PATENT APPLICATION INFORMATION RETRIEVAL

PATENT APPLICATI INFORMAT RETRIEVA

USPTO

PAIR

FAQ

Holp

Feedback

Other Links

E-Business Center Patents

Employee Locator

Class/Subclass GAU Information

Information Contacts

Search results for application number: 09/324,308

Filing or 371(c) Date:	06-02-1999	Class / Sub-Class:	380/044.000
Issue Date of Patent:	-	Location:	TC 2100 CENTRAL 6C09
Examiner Name:	LANIER, BENJAMIN E	Status:	Non Final Action M
Group Art Unit:	2132	Attorney Docket Number:	5577-159
Earliest Publication No:	-	Patent Number:	-
Earliest Publication Date:	-	Customer Number:	20792
Confirmation Number:	1364		

Foreign Priority | Continuity Data | Publication Review

File Contents History

Number	Date	Contents Description
14	12-03-2002	Mail Non-Final Rejection
13	12-01-2002	Non-Final Rejection
12	11-20-2002	Case Docketed to Examiner in GAU
11	08-14-2002	Case Docketed to Examiner in GAU
10	03-02-2002	Case Docketed to Examiner in GAU
9	10-06-2000	Case Docketed to Examiner in GAU
8	09-20-1999	Case Docketed to Examiner in GAU
7	08-09-1999	Information Disclosure Statement (IDS) Filed
6	06-02-1999	Information Disclosure Statement (IDS) Filed
5	08-17-1999	Application Dispatched from OIPE
4	08-13-1999	Application Is Now Complete
3	06-30-1999	Incomplete Application under Rule 53(b) - Filing Date Assigne
2	06-22-1999	Application Scanned
1	06-10-1999	Initial Exam Team nn

HOME | INDEX | SEARCH | SYSTEM ALERTS | BUSINESS CENTER | NEWS&NOTICES | CONTACT US | PRIVACY STATEMENT